

WHAT IS CLAIMED IS:

1. A mobile terminal in a mobile communication system for authenticating a communicating party when communication is performed between the mobile terminal and a device on the side of a network, comprising:
 - 5 authentication processing operation means which, when a request signal requesting operation execution is received from a network device, is for executing authentication processing to check whether said request signal is a request signal from an authorized network device; and
 - 10 operation execution means for executing an operation that is in accordance with said request signal only if authentication that the network device is an authorized network device is obtained.
2. A mobile terminal according to claim 1, wherein said authentication processing means includes:
 - 15 means for storing an identifier and key information of a mobile terminal;
 - 20 a random-number generator for generating any prescribed authentication operation unit for executing a random number;
 - 25 an authentication operation using said key information and random number;
 - 30 creating an authentication request signal, which includes said terminal identifier and random number, and sending this signal to the network device;
 - 35 a receiver for receiving an authentication operation result, which has been obtained by an authentication operation performed on the network side, from the network device; and
 - 40 a comparator for comparing the authentication result computed by the mobile terminal and the authentication result sent from the network device;
 - 45 said operation execution means executes the operation that is in accordance with said request signal upon deciding that the network device is an authorized network device when the compared results agree.
3. A mobile terminal according to claim 1, wherein said authentication processing means executes

authentication processing if a request is one requiring authentication, and said operation execution means executes the operation that is in accordance with said request signal if authentication that the network
5 device is an authorized network device is obtained; and
said authentication processing means foregoes authentication processing if a request is not one requiring authentication, and said operation execution means executes the operation that is in accordance with
10 said request signal.

4. A network device in a mobile communication system for authenticating a network device by comparing, at a mobile terminal, authentication results computed by respective ones of the mobile terminal and network
15 device when communication is performed between these two devices, comprising:

means for sending a signal, which requests that a mobile terminal execute a prescribed operation, to said mobile terminal;

20 a table for storing correspondence between an identifier and key information of a mobile terminal;

a receiver for receiving, from the mobile terminal that has received said request signal, an authentication request signal that includes the
25 identifier and random number of said mobile terminal;

a key-information acquisition unit for acquiring key information, which corresponds to the received identifier of the mobile terminal, from said table;

an authentication operation unit for executing an
30 authentication operation using said acquired key information and said received random number; and

a transmitting unit for transmitting the authentication result to the mobile terminal.

5. A mobile communication system for authenticating a
35 communicating party when communication is performed between a mobile terminal and a device on the side of a network, wherein

the mobile terminal includes:

40 authentication processing means which, when a signal requesting execution of a prescribed operation has been received from a network device, is for sending an authentication request signal to the network device

in order to determine whether said request signal is a request signal from an authorized network device; performing an authentication operation; and comparing result of this authentication operation with result of
5 an authentication operation sent from the network device; and

operation execution means for executing an operation that is in accordance with said request signal only if authentication that the network device
10 is an authorized network device is obtained; and

said network device includes an authentication operation unit for executing an authentication operation based upon an authentication request signal received from said mobile terminal, and sending result
15 of this authentication operation to the mobile terminal.

6. A mobile communication system according to claim 5, wherein the authentication processing means of said mobile terminal includes:

means for storing an identifier and key
20 information of a mobile terminal;

a random-number generator for generating any random number;

an authentication operation unit for executing a prescribed authentication operation using said key
25 information and random number;

an authentication request signal transmitter for creating an authentication request signal, which includes said terminal identifier and random number, and sending this signal to the network device;

30 a receiver for receiving result of an authentication operation obtained by an authentication operation of the network device; and

a comparator for comparing result of the authentication operation performed by the mobile
35 terminal and the result of the authentication operation sent from the network device; and

the authentication processing means decides that the network device is an authorized network device when the compared results agree.

40 7. A mobile communication system according to claim 5, wherein said authentication processing means executes authentication processing if a request is one requiring

authentication, and said operation execution means executes the operation that is in accordance with said request signal if authentication that the network device is an authorized network device is obtained; and

5 said authentication processing means foregoes authentication processing if a request is not one requiring authentication, and said operation execution means executes the operation that is in accordance with said request signal.

10 8. A mobile communication system according to claim 6, wherein said network device further includes:

 means for sending a mobile terminal a request signal requesting execution of an operation;

15 a table for storing correspondence between an identifier and key information of a mobile terminal;

 a receiver for receiving, from a mobile terminal that has received said request signal requesting execution of the operation, an authentication request signal that includes an identifier and random number of
20 said mobile terminal; and

 a key-information acquisition unit for acquiring key information, which corresponds to the received identifier of the mobile terminal, from said table; and

25 said authentication operation unit executes an authentication operation using the key information acquired by said key-information acquisition unit and said received random number, and sending result of the authentication operation to the mobile terminal.

30 9. A mobile communication system according to claim 5, wherein said request signal requesting operation execution is a signal requesting that emission of radio waves be inhibited.

35 10. A mobile communication system according to claim 5, wherein said request signal requesting operation execution is a signal requesting that inhibition of emission of radio waves be cancelled.

40 11. A mobile communication system according to claim 5, wherein said request signal requesting operation execution is a signal requesting that the mobile station make a transition to power cut-off or to a standby operation.

12. A mobile communication system according to claim 5,

wherein said request signal requesting operation execution is a signal requesting disclosure of mobile terminal information possessed by the mobile terminal.

13. A mobile communication system according to claim
5 12, wherein said mobile terminal information is user settings information that a user of the mobile terminal has stored beforehand in a storage unit of the mobile terminal.

14. A mobile communication system according to claim
10 12, wherein said mobile terminal information is status information of the mobile terminal.

15. A mobile communication system according to claim
14, wherein said status information is voltage information indicating residual capacity of a battery
15 of the terminal, or travelling-velocity information measured by a mobile unit, or present-position information detected by a mobile unit.